944-005.5 NC28482

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT APPLICATION OF

LAURI PAATERO

for

METHOD AND SYSTEM TO ALLOW PERFORMANCE OF PERMITTED ACTIVITY WITH RESPECT TO A DEVICE

Express Mail No. EV00525760

METHOD AND SYSTEM TO ALLOW PERFORMANCE OF PERMITTED ACTIVITY WITH RESPECT TO A DEVICE

Technical Field:

The present invention is directed to control of security level functionality in devices and in particular, to control security critical functionality in wireless devices.

Background of the Invention:

Wireless devices and in particular mobile phones continue to have an increasing number of security critical functions built into the devices. Such functions include the ability to sign data, to present protected content using digital rights management (DRM) and similar activities. Some of these features are currently being designed into wireless telephones.

It is contemplated in the future that every mobile phone will have a permanent identity built into the phone. Such an identity can be used to prevent modification of International Mobile station Equipment Identity (IMEI) commonly used with mobile phones. Mobile phones also will have a secret private key for use in public key infrastructure(s) (PKIs). Furthermore, code signing will be used in mobile phones to control execution or installation of security related computer code. Most security critical computer code in mobile phones will be accepted by phone firmware only if it has been signed by a key certified by a Certification Authority (CA root key). In addition, third party developers of applications and the like will from time to time have keys and certificates for creating certain types of programs. It is therefore desirable if these security related issues could be managed at the mobile phone level specific to individual mobile telephones, rather than exclusively at the user (e.g. developer) level.

In the past, it has normally not been possible to effectively prevent an owner or possessor of a mobile phone from replacing code within that mobile phone. The only protection afforded mobile phones in the past has been with regard to remote replacement of code; particularly mechanisms to prevent remote attackers from changing code in phones. However, as noted, there has not been good protection to prevent users of mobile phones from changing the code within the phone. From a practical point of view, it has only been due to the obscurity of the design of mobile phones and the confidentiality of mechanisms within the phones that have made mobile phones relatively difficult to attack by the user of the phone. Unfortunately, such mechanisms also make it difficult for the phone manufacturer to specifically allow certain third parties to have access to at least portions of the code within the phone.

In particular, in many cases a user or some other third party would like to replace code in a mobile phone with other code to circumvent some security mechanism. For example, users might want to replace what is known as International Mobile station Equipment Identity (IMEI) information which is a standardized procedure of equipment manufacturers to identify a mobile station similar to a serial number identification. Thus a user might want to replace the IMEI code in the phone in order to perform illegal services with that phone (such as making telephone calls without payment). At the same time, mobile telephone manufacturers must be able to write code and test that code in order to develop their products efficiently. Thus, the mobile telephone manufacturer may want code having certain modifications used and/or tested by a special group of users with regard to particular mobile phones.

In the past, lowering the security level of a particular mobile phone has been achieved by using some sort of hardware switch or other hardware operation. This type of mechanism cannot be used to efficiently protect against the owner or possessor of a phone from tampering with the phone. In addition, such a mechanism tends to support only a coarse level of security control such as an on/off functionality.

It would be advantageous to allow certain third parties, such as software developers, to have access to specific mobile phones with regard to loading new software code therein, as well as having that software installed on the phone and possibly later executed on the phone. It is to these desired capabilities that the present invention is directed.

It is to address all of these specific issues that the present invention is directed.

Summary of the Invention:

The present invention is directed to a method and apparatus to allow at least one party to perform certain activity(ies) with respect to a device, wherein the device has a role certificate embedded therein, and further wherein that role certificate specifies at least one certain activity which can be activated within the device by at least one party. In particular, the invention is directed to role certificates for mobile phones so as to control security level access by associated phone firmware. In this way the mobile phone is controlled on an individual, per phone basis.

In one implementation, the role certificate controls the acceptance of computer code for use in a specific mobile phone. The computer code can be test code, production code or any type of special code for some operation. The role certificate in this situation indicates what type or types of code can be downloaded, installed and/or run on a mobile phone, thus determining the possible roles that the phone may adopt. The role certificate can indicate not only the types of code that can be downloaded to the phone but also may indicate that such code be written (or delivered) by a specific individual(s) or group, also identified in the role certificate. Different role certificates in the same phone may provide for different activities to be performed on the phone by different entities. Great flexibility is thereby achieved through use of these role certificates.

Another application of the role certificate is control debugging facilities associated with a mobile telephone. Such debugging facilities can be built into the phone or connected to the phone through a port.

The role certificates are in turn controlled by a Certification Authority and thus the certificates can be distributed to third parties to allow third parties to perform specific operations on a mobile phone. For instance, role certificates can be distributed to third party software developers so as to allow those developers to execute low-level debugging of the code on specific mobile phones used for debugging. Such distribution of the role certificates would normally be through bundling of the certificates to the developer with a software development kit (SDK). The role certificate(s) could also be embedded within the device at the time of manufacture or later by the entity that generates the role certificate (typically a root CA).

To verify the role certificate, the mobile phone further stores information regarding the public key corresponding to the private key used by the CA to sign the role certificate. This public key information is typically a hash value of the CA public key. Since this public key information is in a tamper resistant portion of memory within the phone, only a corresponding role certificate can be verified and used in that particular phone once the CA public key is received.

Brief Description of the Drawings:

For a fuller understanding of the nature and objects of the present invention, reference should be made to the following detailed description, taken in conjunction with the following drawings in which:

Figure 1 is a block diagram of a mobile phone device which supports role certificate usage according to the present invention.

Figure 2 is a flow chart showing the steps for implementing a role certificate for a device which allows a third party to perform at least one activity with respect to the device.

Best Mode for Carrying Out the Invention:

As the wireless infrastructure throughout the world has advanced, it has become apparent that mobile phones will have a need for increasing the number of security critical functions that they can perform. Such functionality can include the signing of data, presenting protective content using digital rights management (DRM), and other similar type activities. In the future, every mobile phone will probably have a permanent identity built into the phone. This identity can be used to prevent modification of International Mobile station Equipment Identity (IMEI) based identity which is widely used to identify mobile devices for wireless network service providers. In addition, mobile phones will have a secret key for use in public key infrastructure(s)

(PKIs). The ability to sign code will be used in mobile phones to control execution or installation of security related computer code. Most security critical computer code in mobile phones will be accepted by phone firmware only if it has been signed by key certified by a Certification Authority (CA). In addition, third party developers will, in many situations, have keys and certificates for creating certain types of programs.

The present invention is directed to the use of a mobile phone specific role certificate(s) so as to control security level access to that mobile phone which is enforced by the associate phone firmware. Such a mobile phone specific role certificate provides individual mobile phone security control. Although specifically directed to mobile phones, the method and apparatus of the present invention is generally applicable to any device.

It is important to note that such mobile phone specific role certificates are different from certificates commonly used in network infrastructures. Normally role certificates are given for a certain entity, such as a user or a device, in order to authorize that entity to perform some function to others based upon role membership. Thus, a traditional role certificate might authorize a third party to create test code for a mobile phone. However, in the case of a mobile phone, no one should be allowed to create test code for an arbitrary phone. Thus the present invention uses a mobile phone (device) specific role certificate to allow others to perform some activity on a specific device, such as the mobile phone. When the device has a role certificate such as that used for a development test phone, developers, including third party developers, would typically be allowed to create and run code in that specific test phone without restrictions.

Referring now to Figure 1, a specific mobile phone **10** is shown in a generalized block diagram. It is there seen to contain some form of input/output module **12**, a port **13**, a central processing unit (CPU) **14**, memory **16**, firmware **18**, and an optional debugging facility **20**. Port **13** can optionally connect to an external debugging facility **20'**. A third party (TP) **22** can also interact with the phone through port **13**.

Port **13** is connected to the I/O module for communicating with the outside world. This port can be a wireless antenna, an infrared port, a keyboard, a connector (e.g. an RS 232 port) or other interface. The memory will typically include at least some tamper resistant memory **16′**. In the present invention, a role certificate is issued by a Certification Authority (CA) and as is well-known in the art, such a certificate would contain various components such as those enumerated in ITU-T Recommendation X.509, including the name of the Certification Authority that issued the certificate, a serial number, an expiration date, as well as other information. In particular, the role certificate contains information regarding one or more permitted activities. The role certificate is signed by the CA that created the certificate. Such signing provides the mechanism for allowing an entity (such as the mobile phone or other device) to have confidence in the authenticity of the role certificate since the role certificate can be verified only with the CA's corresponding public key bound to the CA's private key used to sign the role certificate. An overview of such certificates can be found in a Netscape Communications document entitled, "Introduction to Public-Key Cryptology" which can be obtained on the Internet at http://developer.netscape.com/docs/manuals/security/pkin/contents.htm (last updated as of the time of this application filing on 9 October 1998).

The CA public key is typically stored in the tamper resistant portion of memory **16′**. Preferably, a hash of the CA public key is stored in the tamper resistant memory. Then the CA public key, which can be later sent to the device, can be verified by hashing this received CA public key (using the same hashing algorithm used to initially hash the CA public key) and comparing this hash value to that stored in the tamper resistant memory. If the hash values match, the received CA public key is authenticated and can be used to verify the role certificate. The role certificates are typically stored in memory **16**.

Thus an operation security authority such as a mobile phone manufacturer can issue role certificates to, for instance, third party software developers allowing such software developers to perform certain activities with respect to specific mobile phones. The role certificate can be embedded in memory of the device at the time the device is manufactured or may be downloaded later via I/O module **12**. The CA public key(s) (or hash value of such key(s)) would typically be stored in the tamper resistant memory **16′** at the time the device is manufactured. It should be noted that it is possible, if desired, to generate different role certificates using the same CA private key for signing. In such a case, the CA public key within a device can be used to verify any of these role certificates.

It should be noted that a role certificate is typically to be used with one device or possibly a group of devices all associated with the same entity. For instance, a role certificate may be used on a group of mobile phones all owned by a specific company. In each case, the public key (or preferably the hash value of the public key) corresponding to the CA private key used to sign the role certificate is stored in a tamper resistant portion of memory **16′** in each device.

The mobile phone upon receipt of a certificate transmitted to it via I/O module **12** (or previously stored at the time of manufacture) would, through execution of associated firmware code, attempt to verify the certificate using the CA public key. If verified, the phone determines what activities can be performed on itself. If the role certificate can be verified using the CA public key, then a specified activity or activities may be performed on that phone by any third party (if no third parties are identified in the role certificate) or by a specific third party(ies) if they are identified in the role certificate (see below).

Figure 2 is a flow chart showing the various steps for performing generation and use of device specific role certificates such as for use with mobile phones. Thus in step 30, a Certification Authority (CA) generates a role certificate for a specific device, such as a specific mobile phone. The role certificate can be stored in the memory at the time the device is manufactured or it can be distributed to any third party for the third party's use in later communication with the specified mobile phone.

As seen in Figure 2, at step 30, the Certification Authority (CA) generates a role certificate with at least one permitted activity identified within that certificate and optionally including the identity of permitted third parties

(TPs) who may have the right to perform such activities with respect to the device or who have rights with respect to downloading, installing and/or running code in the device. At step 32, the public key of the CA (or preferably the hash value of this pubic key), which corresponds to the CA private key used to sign the role certificate, is stored in the device in the tamper resistant memory **16'**. The storing of the CA public key (or hash value) in memory **16'** can be done at any time prior to or after generation of the role certificate. One or more CA public keys (or hash values of these public keys) can be stored in the device in the tamper resistant memory area and likewise, one or more role certificates can be generated which pertain to a specific device. The CA public key(s) (or hash values) should be stored in tamper resistant memory **16'** in order to prevent TPs from attempting to store their own public keys in the device.

A tamper resistant memory **16'** means some form of memory that can be interrogated to determine if information stored therein has been modified. Firmware **18** can contain code to direct CPU **14** to perform such an interrogation, or such interrogation can be performed remotely via communication with the mobile phone, such as via port **13**.

Other forms of tamper resistance can be used; such as, information storage (or code) obfuscation within the phone or operating system code in the telephone to resist memory changes. Such techniques are not considered to be as efficacious as tamper resistant memory **16'**.

As seen in step 34, the firmware **18** in the device is executed by CPU **14**. One of the functions of the firmware is to control the CPU in order to allow the CPU to use the CA public key (or hash value) stored in tamper resistant memory **16'** in order to attempt to verify a role certificate which has been stored in the device or which has been received by the device from a third party via I/O module **12** and port **13**. If the hash value of the CA public key is stored in tamper resistant memory **16'**, then the firmware causes the CPU to hash a CA pubic key (such as received via port **13**) using same hashing algorithm used to generate the initial hash of the CA public key, and thereby to determine if the hash value matches the hash value in tamper resistant memory **16'**. If the hash values are the same, then the CA public key is used to verify the role certificate (step 36).

At step 36, a decision is made concerning verification of the role certificate. If verified, then at step 38 the permitted activity information, as well as the optional identity of permitted third parties, are parsed from the certificate. This is also performed by CPU **14** under direction of firmware **18**. If the role certificate is not verified, then no activities with respect to the device are permitted (see step 40).

If one or more third parties have been identified in the role certificate, then it is also necessary that the firmware determine if a third party communicating with the device via I/O module **12** matches at least one third party identified in the certificate (step 42). If a match is found, then the parsed activity in step 38 is permitted with respect to the identified third parties. This is shown in step 44. Otherwise, no permitted activities are allowed with respect to the non-identified third parties (see step 46).

With respect to identifying third parties in the role certificate, this can be done by storing a public key of the third party in the certificate and later determining if the received public key from the third party matches that within the certificate. The storing of the third party public key can preferably be done by storing a hash of the third party public key and then performing a hash of the received public key from the third party (using the same algorithm as used to store the hash value of the third party public key in the certificate) so as to determine if the two hashes are identical. If they are, then the identity of the third party is assumed to be correct.

If the third party is allowed to perform permitted activities, the activities can be conducted through the I/O module **12** and port **13**.

It should be noted that the role certificate can identify any type of permitted activity that can be performed on the device, for instance, such activities can provide for the acceptance of computer code from a third party. Thus the role certificate may allow for test code to be received from a third party and for that code to be installed and/or run on the mobile phone. Alternatively, the role certificate can provide for the acceptance of production computer code, again with further allowance of installation and/or running of that code on the specific mobile phone.

Other types of special code can also be provided, depending upon the needs of the development of the phone. Depending upon the activity or activities to be allowed on the specific mobile phone in view of the role certificate, it may be necessary for the mobile phone to further interact with the third party **22** (through, for instance, port **13** - see Figure 1) in order to allow those activities to be performed; such as, the receipt of further data or parameters for use with regard to received code.

As see in Figure 1, the permitted activity may also be the use of a debugging facility **20** within the phone by the TP or to allow the TP to use an external debugging facility **20'** connected to the phone via e.g. port **13**. Thus a flexible and relatively secure method and apparatus have been described which allows the manufacturer of a device to generate role certificates which when read by the device, provide for specified permitted activities(ies) to be performed on the device. The role certificate is therefore the vehicle to allow others to perform such specified activity(ies) on only those device which the manufacturer has previously stored its corresponding CA public key necessary to read the role certificate.

Having described the invention, what is claimed is: